

**Commonwealth of Massachusetts**  
**Center for Health Information & Analysis (CHIA)**  
**Government Agency Application for Data**

*This application is to be used agencies, departments or authorities of the Commonwealth of Massachusetts, as well as federal agencies and departments of the United States of America ("Government Agencies"). Data requests from other states, as well as other political subdivisions of the Commonwealth of Massachusetts must use the Non-Government Agency Application form.*

## I. GENERAL INFORMATION

APPLICANT INFORMATION	
Applicant Name:	
Title:	
Organization:	
Project Title:	
Date of Application:	
Objectives (240 character limit)	

## II. PROJECT SUMMARY

Briefly identify the public purposes for which CHIA data are being sought.

--

## III. FILES REQUESTED

Please indicate the databases from which you seek data, the Level(s) and Year(s) of data sought.

ALL PAYER CLAIMS DATABASE	Level 1 <sup>1</sup> or 2 <sup>2</sup>	Single or Multiple Use	Year(s) Of Data Requested Current Yrs. Available 2009 - 2011
<input type="checkbox"/> Medical Claims	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2	<input type="text"/>	<input type="checkbox"/> 2009 <input type="checkbox"/> 2010 <input type="checkbox"/> 2011
<input type="checkbox"/> Pharmacy Claims	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2	<input type="text"/>	<input type="checkbox"/> 2009 <input type="checkbox"/> 2010 <input type="checkbox"/> 2011
<input type="checkbox"/> Dental Claims <input type="checkbox"/> Member Eligibility <input type="checkbox"/> Provider <input type="checkbox"/> Product	<input type="checkbox"/> Level 2 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 2	<input type="text" value="Select..."/> <input type="text" value="Select..."/> <input type="text" value="Select..."/> <input type="text" value="Select..."/>	<input type="checkbox"/> 2009 <input type="checkbox"/> 2010 <input type="checkbox"/> 2011

<sup>1</sup> Level 1 Data: De-identified data containing information that does not identify an individual patient and with respect to which there is no reasonable basis to believe the data can be used to identify an individual patient. This data is de-identified using standards and methods required by HIPAA.

<sup>2</sup> Level 2 (and above) Data: Includes those data elements that pose a risk of re-identification of an individual patient.

CASEMIX	Level 1 - 6	Fiscal Years Requested
<b>Inpatient Discharge</b>	<input type="checkbox"/> Level 1 – No Identifiable Data Elements <input type="checkbox"/> Level 2 – Unique Physician Number (UPN) <input type="checkbox"/> Level 3 – Unique Health Information Number (UHIN) <input type="checkbox"/> Level 4 – UHIN and UPN <input type="checkbox"/> Level 5 – Date(s) of Admission; Discharge; Significant Procedures <input type="checkbox"/> Level 6 – Date of Birth; Medical Record Number; Billing Number	<u>1998-2012 Available</u> (limited data 1989-1997)
<b>Outpatient Observation</b>	<input type="checkbox"/> Level 1 – No Identifiable Data Elements <input type="checkbox"/> Level 2 – Unique Physician Number (UPN) <input type="checkbox"/> Level 3 – Unique Health Information Number (UHIN) <input type="checkbox"/> Level 4 – UHIN and UPN <input type="checkbox"/> Level 5 – Date(s) of Admission; Discharge; Significant Procedures <input type="checkbox"/> Level 6 – Date of Birth; Medical Record Number; Billing Number	<u>2002-2011 Available</u>
<b>Emergency Department</b>	<input type="checkbox"/> Level 1 – No Identifiable Data Elements <input type="checkbox"/> Level 2 – Unique Physician Number (UPN) <input type="checkbox"/> Level 3 – Unique Health Information Number (UHIN) <input type="checkbox"/> Level 4 – UHIN and UPN; Stated Reason for Visit <input type="checkbox"/> Level 5 – Date(s) of Admission; Discharge; Significant Procedures <input type="checkbox"/> Level 6 – Date of Birth; Medical Record Number; Billing Number	<u>2000-2011 Available</u>

**IV. REQUESTED DATA ELEMENTS [APCD]**

State and federal privacy laws limit the use of individually identifiable data to the minimum amount of data needed to accomplish a specific project objective. Please use the [APCD Data Specification Workbook](#) to identify which data elements you would like to request and attach this document to your application.

**V. REQUESTED DATA ELEMENTS [CASE MIX]**

Please use the CASE MIX DATA SPECIFICATION WORKBOOK to identify which deniable data elements (from Level 2 or above) you would like to request and attach this to your application.

**VI. MEDICAID DATA**

Federal law (42 USC 1396a(a)7) restricts the use of individually identifiable data of Medicaid recipients to uses that benefit the administration of the Medicaid program. If you are requesting Medicaid data from Level 2 or above, please describe in detail why your use of the data benefits the administration of the Medicaid program.

## VII. MEDICARE DATA

Medicare data may be disseminated to state agencies and/or entities conducting research projects that are directed and partially funded by the state if such research projects would allow for a Privacy Board or an IRB to make the findings listed at 45 CFR 164.512(i)(2)(ii) if the anticipated data recipient were to apply for the data from CMS directly. If you are requesting Medicare data, please describe in detail why your proposed project meets the criteria set forth in 45 CFR 164.512(i)(2)(ii). Applicants must describe how they will use the data and inform CHIA where the data will be housed. CHIA must be informed if the data has been physically moved, transmitted, or disclosed.

## VIII. DIRECT PATIENT IDENTIFIERS<sup>3</sup>

State and federal privacy laws may require the consent of Data Subjects prior to the release of any Direct Patient Identifiers. If you are requesting data that includes Direct Patient Identifiers, please provide documentation of patient consent or your basis for asserting that patient consent is not required.

## IX. DATA SECURITY AND INTEGRITY

(Information provided in this section is confidential and not a public record.)

Complete this section for each location where the data will be stored or accessed. If you plan to use an agent/contractor that has access to the data at a location other than your location or in an off-site server and/or database, the agent/contractor should complete this section.

1. Please identify and provide contact information for the person who will be responsible for data security.

2. If your agency has a Written Information Security Program (WISP) or a data sharing agreement/ISA with CHIA that contains data security provisions, please attach the documents and refer to the applicable sections in your response to the questions below.
3. Specify the security measures you will take to prevent unauthorized access to or use of data, including information on access restrictions, handling and storage of data, physical security of the data, audit policies and capabilities, and breach notification policies.

4. Describe how the original data media and subsequent copies of the data will be protected; how mainframe, server or PC data files will be protected; where and how work files are protected; how the data on PCs are protected from access; and how Internet enabled devices will be protected.

5. Describe how you will ensure that data cannot be accessed by portable devices.

---

<sup>3</sup> Direct Patient Identifiers. Personal information, such as name, social security number, and date of birth, that uniquely identifies an individual or that can be combined with other readily available information to uniquely identify an individual.

--

6. Describe any other relevant security and privacy provisions.

--

#### **X. ASSURANCES**

Government Agencies requesting and receiving data from CHIA will be provided with data following the execution of a data use agreement, or pursuant to a specific data sharing agreement referenced herein, that requires the agency to adhere to processes and procedures aimed at preventing unauthorized access, disclosure or use of data.

Government Agencies are further subject to the requirements and restrictions contained in applicable state and federal laws protecting privacy and data security, including but not limited to the Massachusetts Fair Information Practices Act, M.G.L. c. 66A; M.G.L. c. 93H (data breaches); and M.G.L. c. 93I (data destruction).

Government Agencies requesting and receiving data from CHIA must notify CHIA of any unauthorized use or disclosure of CHIA data.

Signature:	
Printed Name:	
Title:	
Agency:	
Date:	